CONSEJOS DE SEGURIDAD EN LA RED

El Internet también conocido como red, web o ciberespacio, es un espacio en el cual buscar información, aprender y trabajar se ha convertido en algo habitual dentro de nuestro día a día; pero a su vez, estos nuevos beneficios dentro del ciberespacio se son lugares donde puede existir fraudes, robos, estafas, engaños o entre otros que conlleven riesgos contra nuestra información, comunicación, actividades económicas e incluso adicción[1]. Por lo que, proteger nuestra red es fundamental para prevenir cualquier tipo de acto lesivo que se pueda generar.

¿Qué es el Internet?

Según la Real Academia de la Lengua se define al Internet como: "Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.".

DIRECTV cuenta con recursos técnicos y logísticos para garantizar la seguridad de la red mediante la que se presta el servicio de acceso a internet. Estos recursos técnicos y logísticos están alineados con los aspectos básicos de seguridad establecidos en las normas ITU-T X.800 "Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT" e ITU-T X.805 "Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo.

Para reforzar la seguridad en el uso del servicio, es responsabilidad de cada suscriptor acatar las siguientes recomendaciones para la navegación segura en internet.

Tips de seguridad

1. **Instalar un antivirus**
   Instalar una aplicación antimalware y mantenerla actualizada puede ayudar a defender tus equipos contra virus y otro malware[2]. Logrando evitar el robo de información, daños parciales o permanentes en tus equipos. Por lo cual, es fundamental mantener actualizado el software y las aplicaciones "antivirus" para ayudar a proteger los dispositivos ante posibles ataques.

[1] (Gobierno de Canarias, 2024)
[2] Malware es un software malintencionado o programa maligno

2. **Contraseñas**
   Evite guardar contraseñas en sus cuentas de correo u otros, con el objetivo de no volver a ingresarlas cada vez que vuelva al sitio web o aplicación determinado.

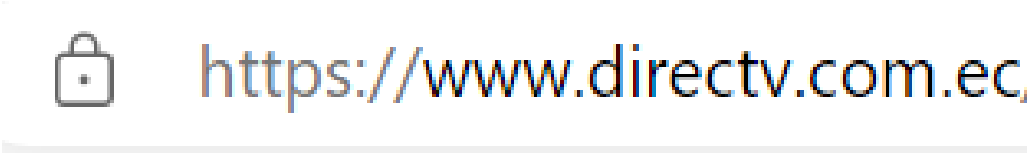
   Se sugiere mantener actualizadas las contraseñas cada seis meses. Las cuales deberán contener como mínimo 8 caracteres, con una configuración entre números y letras de preferencia no consecutivos, con al menos un signo o carácter especial.

3. **Correo electrónico**
   Se recomienda evitar compartir información confidencial a correos desconocidos, no responder mensajes de cadenas publicitarias o sean cadenas maliciosas que contengan archivos malintencionados que puedan afectar a su equipo o a terceros.

   Procure no abrir, contestar o reenviar correos enviados por un destinatario desconocido.

4. **Descarga de Archivos**
   Se recomienda descargar y ejecutar archivos únicamente desde sitios reconocidos y confiables. En caso de correo electrónico, es esencial asegurarse de que provenga de una fuente confiable y legítima.

5. **Ingresar a páginas web que garanticen seguridad al momento de navegar**
   Se sugiere verificar que los sitios web que se visiten mantengan un "candado de seguridad" *(icono)* al inicio de la dirección URL. Para una mejor comprensión se indica el siguiente ejemplo:



6. **Cerrar sesión en los dispositivos.**
   Se recomienda finalizar sesión en los dispositivos de las cuentas abiertas una vez que las mismas ya no se estén utilizando.

7. **Seguridad de su red wifi**
   Evite compartir la contraseña de su red wifi con personas desconocidas o dejarla a simple vista del público en general. Se recomienda que la contraseña de su red wifi se mantenga actualizada cada 6 meses para evitar infiltraciones no deseadas.

8. **Evita conectarse a redes de acceso públicas**
   Son redes de acceso público en las que no se requiere de una contraseña para poder navegar dentro del internet y, como su nombre lo determina son de uso público. Razón por la dentro de estas redes te puedes encontrar con ciberdelincuentes que buscan obtener información confidencial, así como datos personales con la finalidad de infectar los equipos con malware, acceder a informar como números de tarjetas de crédito o débito, escanear comunicaciones y especiar.

   Por lo cual, la ARCOTEL a través del Centro de Respuesta a Incidentes informáticos de ARCOTEL (EcuCERT)[3] advierte de estos riesgos y recomienda medidas de seguridad que se pueden tomar durante el uso de redes wifi de acceso público debido a su alto grado de riesgo, como son: instalar de antivirus y un antimalware, y evitar realizar transacciones a sitios que requieran identificación con calves de acceso.

Referencias

ARCOTEL. (- de - de 2021). *ARCOTEL*. Recuperado el 11 de Marzo de 2024, de https://www.arcotel.gob.ec/protocolo-de-seguridad-para-evitar-la-suplantacion-de-identidad/

Gobierno de Canarias. (- de - de 2024). *Gobierno de Canarias, Cnsejeria de Educación, Formación Prosional, Actividad Física y Deportes*. Recuperado el 06 de Marzo de 2024, de https://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/riesgos-asociados-al-uso-de-las-tecnologias/riesgos/

[3] (ARCOTEL, 2021)